Mandatory principles

January 2016

Nestlé

Good Food, Good Life

Information Security Code for Nestlé Suppliers

Issued by
Nestlé Information Security

Target group
Suppliers and subcontractors of Nestlé Česko s. r. o. (hereinafter „Nestlé“)

Revised by
Information Security Manager
LGO Manager
Corporate Affairs Director
Legal Division Director
Procurement Director

Approved by
General Director Nestlé Česko, s. r. o, January 2016

Version
1.0

Copyright
All rights belong to Nestlé Česko, s. r. o.

Introduction to the Information Security Code for Nestlé Suppliers

1. Purpose

The Nestlé Information Security Code for Suppliers defines the minimum level of information security, to be respected and adhered to by the suppliers and their subcontractors (hereinafter the „Supplier“), as required by Nestlé.

This document contributes to the continuous implementation of the commitment of Nestlé to maintain a secure internal and external information environment resulting from international safety standards, such as ISO/IEC 27001 (hereinafter referred to as „information security management system“).

2. Scope

The Information Security Code sets forth expectations for suppliers with whom Nestlé does business, including its parent, subsidiary or affiliate entities, including all employees (including permanent, temporary, contract agency and migrant workers), upstream suppliers and other third parties, as well as all others cooperating with the Supplier in Nestlé data processing. The Supplier shall take full responsibility for the subcontractors and other third parties whose services it uses to comply with the obligations of the Nestlé Supplier originating from this Code. It is the responsibility of the Supplier to expand its technological development in connection with information security, employee awareness and conscientiously verify compliance of their environment with this Code, among its employees, agents and lower tier suppliers, wherever relevant.

3. Compliance

Nestlé expects that the Supplier shall comply with all applicable laws and regulations, and above all those regulating the pillars described herein, and will seek to comply with international safety standards and best practices. Additionally, in line with the management of suppliers within the information security management system in accordance with the Nestlé Supplier Code, Nestlé reserves the right to verify compliance of actions and procedures of the Supplier with the Information Security Code and the conditions arising out of the specific contractual relations between Nestlé and the Supplier through internal or external evaluation and audit mechanisms and require the implementation of changes resulting from audit requirements or requirements supplementing the Nestlé information security management system. The supplier is obligated to remedy the identified deficiencies at own expense.

4. Continuous Improvement

Nestlé recognizes that achieving the standards established in this Code is a dynamic process, and encourages the Supplier to continually improve their processes and operations. Should an improvement be required, Nestlé will provide support to ensure the enhancement of mutual information security.

5. Application

The acknowledgement of the Information Security Code is a prerequisite, as well as in the case of the Supplier Code, for the conclusion of every Nestlé contract for supply. By accepting the Purchase Order with reference to the Information Security Code, the Supplier commits that all its processes and operations are in accordance with the provisions contained in this Code.

The pillars of the Information Security Code are complementary to and do not substitute security measures contained within any legal agreement or contract between the Supplier and Nestlé.

Pillars of Nestlé Information Security Code for Suppliers

1. Transparent information relations

Openness and transparency are key to creating a sense of confidence and credibility in the transfer of data between business entities. Nestlé expects the Supplier to comply with basic concepts to avoid conflicts of interest and abstain from corruption activities in connection with Nestlé.

The Supplier under no circumstances shall tolerate corruption behaviour and strives to ensure that the employees, subcontractors or representatives do not accept, offer or give out bribes, unauthorized gifts or other improper payments or other benefits to customers, public officials or third parties.

The Supplier shall keep in mind the applicable laws, especially the Act on Protection of Competition. The Supplier shall not conclude agreements contrary to the rules of competition with competitors, suppliers or customers and shall not abuse any potential dominant position in the market. In connection with this Code, the Supplier shall particularly care about ethical handling of data in their electronic exchange amongst the commercial entities.

2. Data Protection

By observing this Code, the Supplier undertakes to set up an adequate level of managed data protection corresponding to the nature and purpose of the data for which these data are used.

The Supplier shall be able to protect all data that may, if made public or disclosed, cause significant damage to the reputation of or financial loss to Nestlé.

The Supplier shall respect the confidential information, know-how, operational and business secrets of Nestlé. Such information shall not be provided to third parties without the prior express written consent of Nestlé and shall not be disseminated in any other unauthorized manner.

Data protection shall be ensured during transmission over public networks as well as private network of the Supplier. Data protection also applies to the Supplier‘s data storage.

Data must be protected against damage, unauthorized use, and must not be disturbed in terms of availability, confidentiality and integrity. The Supplier shall ensure that the data is properly stored, and if requested by Nestlé, returned back to Nestlé

3. Protection of personal and sensitive data

Nestlé expects that the Supplier shall comply with all applicable laws and regulations regarding the protection of personal data and sensitive data. These are all personal and sensitive data that are processed by the supplier in connection with services provided to Nestlé.

The Supplier shall ensure that access to Nestlé personal and sensitive data and other confidential data is provided only to authorized users and is required to verify the identity of the authorized persons.

The Supplier shall ensure that Nestlé’s personal data and sensitive information are not kept for a longer period than is necessary for the provision of services, unless the continued storage of Nestlé’s personal data is required by law.

Upon request, the Supplier shall be able to provide a confirmation of the destruction of Nestlé’s personal or sensitive data.

4. Ability to respond

The Supplier has established mechanisms to detect information security events and incidents involving Nestlé data. The Supplier shall be able to report these events and incidents as soon as possible to Nestlé to reduce the potential overall impact.

The Supplier undertakes not to issue any press release or public announcement related to a completed or incomplete incident or event involving any Nestlé data, or information related to Nestlé, without obtaining consent from Nestlé, unless explicitly required by law or any other legislation.

Reporting violations

The supplier shall report any suspected violations of regulations, laws and the Information Security Code for Suppliers. Violations should be reported to the contact person in Nestlé or may be reported confidentially by using one of the available channels:
e-mail address in case of suspicion of an event or incident:
information.security@cz.nestle.com.

Hotline for very serious incidents:
+41 21 924 22 22.

Acknowledgement

Supplier's Acknowledgement (If required by the Nestlé's Purchasing division)

We, the undersigned, hereby confirm that:

- We have received and taken due notice of the contents of the Nestlé Information Security Code for Suppliers, dated 2016, published by Nestlé Česko s. r. o.
- We are aware of all the relevant laws and regulations of the countries in which our company operates and Nestlé Česko s. r. o.
- We shall report to Nestlé S.A any case of suspected violation of the Information Security Code for Suppliers.
- We shall comply with the requirements of the Information Security Code for Suppliers.
- We shall inform all our employees / subcontractors of the contents of the Nestlé Information Security Code for Suppliers and ensure that they observe the measures contained therein.
- We hereby authorise the company Nestlé Česko s. r. o. or any organizations acting on behalf of Nestlé Česko s.r.o. to carry out audits with or without notice at our premises and the business premises of our subcontractors at any time to verify compliance with the Nestlé Information Security Code for Suppliers.
- We are aware that if we do not adhere to basic principles of this Nestlé Information Security Code for Suppliers, Nestlé reserves the right to take appropriate legal action and to reconsider further cooperation with us.

Name of Company

Signature/Stamp

Name and function

Entry in the Commercial Register/Corporate identity/Code/Number

Date and place

This document must be signed by an authorized representative of the Supplier and returned to the Nestlé Purchasing division.